Riversdale Primary School

A nurturing, ambitious and values led school.

SOCIAL MEDIA POLICY

DATE: 1st June 2026

REVIEW DATE: 30th May 2029

PURPOSE

Riversdale Primary School recognises that social media can be a positive way to celebrate school life, communicate key messages, strengthen relationships with the school community and promote the school to prospective families.

This policy sets out how the school uses social media safely, responsibly and professionally. It also explains expectations for staff, governors, volunteers, parents, carers and other members of the school community when using social media in ways that may affect the school, its pupils, staff or reputation.

Safeguarding children is the school's first priority. All use of social media must protect pupils' welfare, privacy, dignity and safety.

OFFICIAL SCHOOL SOCIAL MEDIA ACCOUNT

Riversdale Primary School's only official social media account is:

Instagram: @RiversdalePrimary

The school does not currently operate official Facebook, X/Twitter, TikTok, Snapchat, WhatsApp, YouTube or other social media accounts, though the PTC/Friends of Riversdale operate their own Instagram and oversee the parent WhatsApp groups.

Any account using the school's name, logo, images or identity without written permission from the Headteacher is not an official school account.

The school website, Weduc and Arbor remain the school's primary formal communication channels. Instagram is used to celebrate and promote school life, not as the main method for communicating essential information.

LEGAL AND STATUTORY FRAMEWORK

This policy has been written with regard to:

- Keeping Children Safe in Education, which sets out schools' safeguarding responsibilities, including online safety and the need to protect children from harm online;
- Working Together to Safeguard Children;
- Education Act 2002, particularly the duty to safeguard and promote the welfare of children;
- Children Act 1989 and Children Act 2004;
- Data Protection Act 2018 and UK GDPR;
- Equality Act 2010;
- Computer Misuse Act 1990;
- Malicious Communications Act 1988 and Communications Act 2003, where relevant to harmful, threatening or abusive online communication;
- Online Safety Act 2023, particularly the wider national framework for reducing online harm;
- DfE guidance on data protection in schools, including advice that schools should not publish photos or videos of pupils who should not be publicly identified, such as pupils with safeguarding concerns or court orders.

The school will also have regard to DfE filtering and monitoring standards and online safety expectations. Schools are expected to have appropriate filtering and monitoring arrangements in place to help protect pupils from harmful online content.

AIMS

Through this policy, Riversdale Primary School aims to:

- celebrate pupils' learning, achievements and wider school life;
- promote the school's vision, values and ethos;
- strengthen positive communication with families and the local community;
- protect pupils, staff and families from safeguarding, privacy and reputational risks;
- ensure that images and information are shared lawfully and appropriately;
- make clear who may post on behalf of the school;
- prevent the misuse of the school's name, logo, identity or images;
- ensure concerns linked to social media are responded to promptly and appropriately.

PRINCIPLES

All use of social media connected to Riversdale Primary School must be:

- safe;
- lawful;
- respectful;
- professional;
- inclusive;
- accurate;
- proportionate;
- consistent with the school's safeguarding and data protection responsibilities.

The school will not publish content that:

- identifies pupils who should not be publicly identified;
- compromises safeguarding arrangements;
- reveals confidential or sensitive information;
- embarrasses, humiliates or ridicules pupils, staff or families;
- includes inappropriate comments, images, music, hashtags or links;
- could damage the reputation of the school or school community;
- breaches copyright, data protection or confidentiality requirements.

MANAGEMENT OF THE SCHOOL INSTAGRAM ACCOUNT

The official school Instagram account will be managed by authorised staff only.

Authorised users may include:

- the Headteacher;
- members of the Senior Leadership Team;
- other staff specifically authorised by the Headteacher.

No other member of staff, governor, volunteer, parent, carer or pupil may post on the official school Instagram account.

The Headteacher has overall responsibility for the account and may remove content, restrict access or suspend posting at any time.

Login details must be kept secure. Passwords must not be shared with unauthorised users and should be changed when staff with account access leave the school or no longer require access.

Where possible, school social media accounts should be accessed through school-managed devices or secure school systems.

CONTENT PUBLISHED BY THE SCHOOL

The school may use Instagram to share:

- examples of learning;
- school events;
- curriculum enrichment;
- assemblies and celebrations;
- sports, arts and music activities;
- values and personal development work;
- reminders or signposting to information already shared through formal school channels;
- information for prospective families;
- community messages approved by the school.

The school will ensure that posts are accurate, appropriate and aligned with the school's ethos.

Instagram will not normally be used for:

- urgent safeguarding messages;
- individual pupil matters;
- complaints;
- confidential communication;
- detailed operational messages that should be sent through Weduc, Arbor, email, letter or the school website.

PHOTOGRAPHS AND VIDEOS OF PUPILS

The school will only publish photographs or videos of pupils where this is lawful, appropriate and consistent with the school's consent and safeguarding arrangements.

Before publishing pupil images, staff must check:

- whether parental consent is in place;
- whether the pupil has objected or appears uncomfortable;
- whether the image could create a safeguarding risk;
- whether the pupil is subject to any restriction, court order or safeguarding arrangement that means they must not be identified;
- whether the image reveals personal or sensitive information;
- whether the image is dignified and appropriate.

The Information Commissioner's Office explains that schools may set their own rules around photography at events, and that asking parents not to post images of other people's children on social media is a sensible policy position.

The school will not publish:

- pupils' full names alongside photographs or videos;
- personal contact details;
- home addresses;
- class lists;
- information about a pupil's medical, SEND, safeguarding or family circumstances;
- images that show pupils in distress, embarrassment or vulnerable situations;
- images of pupils who do not have appropriate consent for publication;
- images that reveal the identity or location of pupils who should not be publicly identified.

Group photographs may be used where appropriate, but consent and safeguarding checks still apply.

CONSENT AND WITHDRAWAL OF CONSENT

The school will obtain and record parent/carer consent for the use of pupil images in line with the school's Photographic and Video Images Policy and Data Protection Policy.

Parents and carers may withdraw consent at any time by contacting the school office. The school will act on withdrawal of consent for future publications as soon as reasonably practicable.

Where an image has already been published, the school will consider whether it is reasonable and practical to remove it, taking account of safeguarding, data protection and technical limitations.

Even where consent has been given, the school may decide not to publish an image if there is a safeguarding, welfare or reputational concern.

SAFEGUARDING

Safeguarding is paramount in all decisions about social media.

Staff must not publish or approve any post that could:

- identify a pupil who is at risk of harm;
- reveal a pupil's location where this could create risk;
- identify pupils subject to court orders, care arrangements or other protective measures;
- expose pupils to contact from unknown adults;
- enable grooming, harassment or exploitation;
- contribute to bullying, discrimination or online abuse;
- compromise the security of the school site.

If there is any doubt about whether content is safe to publish, staff must consult the Designated Safeguarding Lead before posting.

Any safeguarding concern arising from social media must be recorded and managed in line with the school's Safeguarding and Child Protection Policy.

STAFF USE OF SOCIAL MEDIA

Staff are expected to maintain professional boundaries online at all times.

Staff must not:

- communicate with pupils through personal social media accounts;
- accept or send friend/follow requests to current pupils from personal accounts;
- send private messages to pupils through social media;
- use personal accounts to discuss confidential school matters;
- post comments, images or videos that could bring the school into disrepute;
- make derogatory, offensive or unprofessional comments about pupils, parents, carers, colleagues, governors or the school;
- publish images of pupils on personal social media accounts;
- use the school's name, logo or branding on personal accounts without permission;
- create class accounts or unofficial school accounts.

Staff who have personal connections with families or pupils outside school, for example through family friendships or community groups, should ensure that boundaries remain appropriate and transparent. Any situation that could create a safeguarding or professional boundary concern should be discussed with a senior leader.

Staff should ensure that privacy settings on personal social media accounts are appropriately managed. However, staff should be aware that privacy settings do not guarantee confidentiality and that online content can be copied, shared or screenshotted.

PROFESSIONAL ACCOUNTS

Staff may maintain professional social media accounts that are separate from the school. However, they must not use such accounts to post identifiable images of Riversdale pupils or confidential school information.

Professional accounts must not give the impression that they are official Riversdale accounts unless this has been explicitly approved by the Headteacher.

Staff must not use professional accounts to communicate privately with pupils.

PARENT AND CARER USE OF SOCIAL MEDIA

The school recognises that parents and carers use social media to communicate and share information. The school asks parents and carers to use social media responsibly and respectfully.

Parents and carers must not use social media to:

- post images or videos of other people's children without permission;
- make abusive, threatening, discriminatory or defamatory comments about pupils, staff, governors, parents, carers or the school;
- raise complaints about individual pupils or staff members;
- share confidential information about school matters;
- identify pupils involved in behaviour, safeguarding or pastoral incidents;
- contact staff through personal social media accounts;
- create accounts that appear to represent the school without permission;
- use the school logo, branding or images without permission.

Concerns or complaints should be raised directly with the school through the appropriate channels, not through social media. Where a matter is a formal complaint, it should be handled through the school's Complaints Procedure.

COMMENTS, MESSAGES AND TAGGING

The school may limit, moderate or disable comments on Instagram posts where this is necessary to protect pupils, staff or the school community.

The school will not use Instagram direct messages as a formal communication channel. Parents and carers should contact the school through Weduc, email, telephone or the school office.

The school may remove, hide or report comments that are:

- offensive;

- abusive;
- discriminatory;
- threatening;
- defamatory;
- political or campaigning in a way that is inappropriate for the school account;
- commercial advertising or spam;
- likely to identify or embarrass a pupil, family or member of staff;
- linked to a safeguarding or confidentiality concern.

The school may block or restrict users who repeatedly breach these expectations.

PUPIL USE OF SOCIAL MEDIA

Primary-age pupils are below the minimum age for many social media platforms. Instagram's minimum age is 13. Parents and carers are responsible for supervising their child's social media use outside school and ensuring that age restrictions are followed.

The school teaches pupils about online safety through the curriculum, including:

- keeping personal information private;
- respectful online behaviour;
- cyberbullying;
- reporting concerns;
- consent and image sharing;
- recognising unsafe contact;
- knowing where to get help.

Where online behaviour outside school affects pupils' safety, wellbeing, relationships or behaviour in school, the school may respond in line with its Behaviour and Anti-Bullying Policy, Online Safety Policy and Safeguarding and Child Protection Policy.

CYBERBULLYING AND ONLINE ABUSE

Cyberbullying is the use of digital technology to deliberately upset, threaten, humiliate, harass or intimidate another person.

The school will take cyberbullying seriously, particularly where it affects pupils, staff, families or the safe running of the school.

This may include:

- pupil-to-pupil cyberbullying;
- abusive messages about staff;
- harmful group chats;
- sharing images without consent;
- impersonation accounts;
- harassment;
- discriminatory abuse;
- online threats.

Concerns should be reported to the school as soon as possible. Families are encouraged to keep evidence, including screenshots, dates, times, usernames and links.

Where appropriate, the school may advise families to report content to the platform or to the police.

MOBILE PHONES, CAMERAS AND RECORDING ON SCHOOL SITE

Personal mobile phones, cameras and recording devices must be used in line with the school's safeguarding, online safety and data protection procedures.

Parents, carers and visitors must not take photographs or videos on the school site unless the school has given permission.

At school events, the school may allow parents and carers to take photographs or videos for personal use. However, parents and carers must not post images or videos of other people's children on social media without permission.

Staff must not use personal mobile phones to photograph or video pupils, unless this is in an exceptional situation and has been authorised in line with school procedures.

CONFIDENTIALITY AND DATA PROTECTION

All social media use must comply with the school's Data Protection Policy and UK GDPR.

Staff must not post or share:

- personal data about pupils, families, staff or governors;
- confidential school information;
- safeguarding information;
- medical information;
- SEND information;
- behaviour information;
- assessment data;
- internal documents;
- information from CPOMS or other school systems;
- private correspondence.

The school will ensure that personal data published on Instagram is limited, necessary and appropriate.

USE OF THE SCHOOL NAME, LOGO AND BRANDING

The school's name, logo, photographs, branding and published materials must not be used on social media without permission from the Headteacher.

This includes use by:

- staff;
- governors;
- parents and carers;
- pupils;
- volunteers;
- external organisations;
- clubs or hirers;
- community groups.

Where unauthorised use of the school's identity is identified, the school may request that it is removed and may take further action where necessary.

EXTERNAL ORGANISATIONS, VISITORS AND MEDIA

External organisations, visitors, contractors and community partners must not publish images or information about Riversdale pupils or school activities without prior permission from the school.

Where external organisations attend school events, staff must ensure that expectations around photography, filming and social media are made clear in advance.

Local media involvement must be approved by the Headteacher. Parent/carer consent and safeguarding checks must be completed before any pupil is photographed, filmed or interviewed for media publication.

INAPPROPRIATE, ILLEGAL OR HARMFUL ONLINE CONTENT

There are no circumstances in which staff, governors, volunteers or visitors should access, create, store, share or distribute illegal content.

If illegal or suspected illegal content is identified, including indecent images of children, staff must not investigate, download, forward or share the material. The matter must be reported immediately to the Designated Safeguarding Lead or Headteacher, who will seek appropriate advice and contact the police or local authority designated officer where required.

Where unsuitable but not clearly illegal content raises concerns about a staff member's suitability to work with children, this will be managed in line with safeguarding procedures, staff conduct procedures and local authority advice.

BREACHES OF THIS POLICY

Breaches of this policy may be dealt with under the relevant school procedure.

For staff, this may include:

- safeguarding referral;
- low-level concern recording;
- disciplinary action;
- referral to the local authority designated officer;
- referral to the police, where appropriate;
- referral to the Disclosure and Barring Service or Teaching Regulation Agency where required.

For pupils, breaches may be dealt with under the Behaviour and Anti-Bullying Policy, Online Safety Policy and Safeguarding and Child Protection Policy.

For parents, carers or members of the public, the school may:

- request removal of content;
- restrict comments or access to the school Instagram account;
- block or report accounts;
- use the Complaints Procedure where relevant;
- seek legal, local authority or police advice where necessary.

For governors or volunteers, breaches may be considered under the relevant code of conduct or safeguarding procedures.

MONITORING AND REVIEW

The Headteacher and Designated Safeguarding Lead will monitor the school's use of Instagram and ensure that it remains safe, appropriate and aligned with this policy.

This policy will be reviewed annually, or sooner if:

- safeguarding guidance changes;
- data protection guidance changes;
- the school opens or closes a social media account;
- there is a significant social media incident;
- the governing body requests a review.